

invention can be embodied in a multitude of different ways as defined and covered by the claims.

[0019] **FIG. 1** illustrates an exemplary smart card **100** that may be used to verify biometric information and sign a data item. Although the following text describes the use of a smart card **100**, the processes that are performed by the smart card **100** can be integrated with any type of portable electronic device, for example a wireless handheld device. Furthermore, it is noted that the portable electronic device can comprise software, hardware, or a combination thereof. The smart card **100** receives the biometric information via a biometrics interface **110** and then processes the biometric information with a biometrics processor **114**. The smart card **100** also includes a central processing unit (CPU) **118**, a random access memory/read only memory (RAM/ROM) **122**, a cryptosystem **126**, and a card reader interface **130**. The cryptosystem **126** may include an electrically erasable programmable read only memory (EEPROM) **134** and a cryptosystem processor **138**. The EEPROM **134** may contain a unique identifier, e.g., card serial number, associated with the smart card **100** which may be used in key generation. These various components may communicate over a shared bus. It is noted that, depending on the embodiment, other hardware configurations may be used. For example, in one embodiment, the biometrics processor **114**, the CPU **118**, and the cryptosystem processor **138** can be integrated into a single processor.

[0020] **FIG. 2** is a block diagram illustrating the process flow of the smart card **100** during an enrollment mode. **FIG. 2** also illustrates certain functionalities that may be embodied as software modules that are executed by the hardware shown in **FIG. 1**. Insofar as functionality, the smart card **100** comprises a biometric data analyzer **200**, a random number generator **204**, an encryption module **208**, and a one-way hash function **212**. The biometric data analyzer **200**, the random number generator **204**, the encryption module **208** and the one-way hash function **212** may be implemented in either hardware or software. In one embodiment, the biometric data analyzer **200** is associated with the biometrics processor **114** and functions **204**, **208** and **212** are associated with the cryptosystem **138**.

[0021] In one embodiment of the invention, the biometric data analyzer **200** executes on the biometrics processor **114** (**FIG. 1**). In the enrollment mode, the biometric data analyzer **200** receives biometric data **216** from a user and triggers the random number generator **204** to create a public key **220** and a private key **224**. The private key **224** is stored in a tamper-resistant component on the smart card **100**. The public key is transmitted to an external device, such as a computer, via the card reader interface **130**.

[0022] In one embodiment, once a set of biometric parameters is selected, a graphical distribution of identifications is made in n-dimensions. Registration is conducted against known templates in dependence upon the selected parameters.

[0023] Once registration is complete, a single point is determined having coordinates equal to each of at least some of the registration results. Alternatively, the point has coordinates determined in dependence upon the registration results but not equal thereto. Plotting the point results in a point plotted in n-dimensional space. The biometrics processor **114** then determines a probability distribution for the

selected parameters. Alternatively, this is performed prior to the registration process for biometric information samples. Further, alternatively the probability distributions are determined or approximated in advance and stored in non-volatile memory such as ROM **122**.

[0024] **FIG. 3** is a block diagram illustrating the process flow of the smart card **100** during a signing mode. In the signing mode, a clear message **230** is transmitted to the smart card **100** via the card reader interface **130** (**FIG. 1**). For authentication purposes, as is explained in further detail below, the one-way hash function **212** creates a message digest **232** based upon the content of the clear message **230**. The encryption module **208** then encrypts the message digest with the private key **224** to create a digital signature **234**. The digital signature **234** is then appended to the clear message **230**, and is transmitted to an external device, such as a computer via the card reader interface **130**.

[0025] Before any message is sent, the user must re-provide the biometric data **216** for user verification. Given an n-dimensional plot defined by a boundary function and a single point, a comparison determines whether or not the point falls below or above the function and optionally within or outside other known ranges. Stated differently, the point is analyzed to determine whether it falls within a suitable region wherein region is defined as an n-dimensional region having at least some known boundaries. When the point falls within a predetermined or suitable region, the individual is identified. When the point falls outside the predetermined or suitable region, the individual is not identified.

[0026] In another approach, actual features are computed from the measurements and combined to a vector of feature values, called a feature set. For a comparison of two biometric data only the two feature sets are compared. To compare two feature sets, each feature is compared and weighted separately. To find good weightings for this comparison can be difficult, and an artificial neural net approach may be used for this purpose. The arithmetic differences between each two corresponding features from all features of the feature sets is calculated and fed into the neural net. There they are weighted internally and an output is calculated which gives a value to be interpreted as the probability whether the two sets match. A well-trained neural net can classify not only sets used during training but also novel sets presented the first time. Once the neural net is trained and the acceptable range of output values is determined the identification can readily be made. If the output falls within this range, the individual is identified, if it is outside the range, the individual is not identified.

[0027] Although current biometric devices and algorithms based on these approaches now routinely achieve acceptable levels of false acceptance, false rejection and failure to enroll rates, a limitation of all biometric devices remain the possibility for a fraudulent user to capture and fake the input device or to access and replay the biometric data channels. To overcome this limitation, the smart card **100** converts the biometric data **216** into a digital signature **234** in a tamper-proof way.

[0028] There are two types of cryptographic systems in which digital signatures have been used: symmetric and asymmetric cryptosystems. In symmetric (conventional) cryptography the sender and recipient of a communication share a secret key. This key is used by the sender, the